**Cyber Security Advisories**

**Date: 30 November 2024**

1. **TA-MAW-2024-11-18-002**

RustDoor aka Thiefbucket, a Remote Access Trojan (RAT), is written in the Rust language, targeting macOS systems, with a particular focus on cryptocurrency firms. The malware is typically distributed by masquerading as legitimate software updates, such as updates for Microsoft Visual Studio, as job offers packaged in ZIP archives. These archives contain malicious shell scripts that, when executed, retrieve the RustDoor implant from attacker-controlled domains. To avoid detection, the scripts may also display decoy files to mislead users.

**Impacts:**

* Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.
* System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Hashes:**

51a88646f9770e09b3505bd5cbadc587abb952ba

5ec7497107478f08ca5018bf659f9340880c059c

a246db8fe1a4f385ed5e2eed5087a60fd2be6b5a

254aad39a432ff0df2ce35cc4ff3578afe1dc1df

f669fba857401406db6b35958d5f57d9d8030f56

f11ca6e92a3f2af3590021d1475a740e6246347e

c401c8aafc28317828f6b648a3abf6e01d05efae

**Domains:**

taurihostmetrics.com

wiresapplication.com

juchesoviet48.com

**IPs:**

185.234.216.180

139.59.182.234

62.204.41.73

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-18-003**

Reference is made to earlier advisories on the AsyncRAT malware.

ASYNCRAT, a backdoor written in .NET, uses a unique binary protocol to communicate over TCP. The backdoor has the ability to run shell commands and download plugins, which may be kept in the registry or run immediately in memory. The downloaded Plugins can add features like file transfer, keylogging, video recording, screenshot capture, and cryptocurrency mining. Additionally, ASYNCRAT provides a plugin that targets login credentials kept by web browsers running on Chromium and Firefox. Adversary after execution, establishes communication with the Command & Control (C2) server and allows remote control of the compromised systems.

**Impacts:**

* Remotely control of the compromised systems.
* Execute remote commands, Log keystrokes, Exfiltrate data and deploy additional malware.
* AsyncRAT can be used to spread laterally across the network, potentially infecting other systems and creating a broader security breach.
* AsyncRAT often includes features to evade detection and maintain persistence in the infected system, making it challenging to remove and recover from the infection.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

103.195.100.105

207.231.111.82

45.88.186.211

78.161.46.79

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-11-18-006**

It has been observed that APT36 a.k.a. Transparent Tribe is deploying CrimsonRAT, a Remote Access Trojan (RAT) for cyber-espionage activities, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

**Common Features of APT36 Threat Actor:**

* Spear-Phishing (highly targeted and convincing phishing emails to trick victims)
* Information Theft (documents, credentials, and personal data)
* Remote Access
* Credential Harvesting
* Data Exfiltration
* Persistence Mechanisms

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

qhev18.duckdns.org

**IP:**

167.160.167.18

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-11-19-009**

It has been observed that threat actors are exploiting the Remote Command Execution (RCE) vulnerability in the Palo Alto PAN-OS management interface, against a limited number of firewall management interfaces which are exposed to the Internet.

Devices whose access to the Management Interface is not secured as per our recommended best practice deployment guidelines are at increased risk.

**Steps to identify your devices:**

**Step 1.** To find your assets that require remediation action, visit the Assets section of the Customer Support Portal at https://support.paloaltonetworks.com (Products → Assets → All Assets → Remediation Required).

**Step 2.** The list of your devices with an internet-facing management interface discovered in our scans are tagged with PAN-SA-2024-0015. If no such devices are listed, it indicates our scan did not find any devices with an internet-facing management interface for your account.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

136.144.17.\*

173.239.218.251

216.73.162.\*

Note: These IP addresses may represent third party VPNs with legitimate user activity originating from these IPs to other destinations. Blocking these IPs could interfere with the organization’s operations. Therefore, network administrators are encouraged to monitor these IPs closely. If any traffic is detected directed towards them, a thorough threat-hunting process should be initiated to facilitate early containment of potential infections.

**HASH:**

3c5f9034c86cb1952aa5bb07b4f77ce7d8bb5cc9fe5c029a32c72adc7e814668 (web shell)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-19-006**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

aadhar.jharkhand.gov.in.2024.es

www.www.ftp.cscgov.info

www.karnataka.gov.inwww.bteresults.net

kerala.gov.in.email

assam.gov.in.holiday

\*.gov.in.2024.es

\*.cscgov.info

\*.gov.inwww.bteresults.net

\*.gov.in.email

\*.gov.in.holiday

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-19-007**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

aadhar.jharkhand.gov.in.2024.es

www.www.ftp.cscgov.info

www.karnataka.gov.inwww.bteresults.net

kerala.gov.in.email

assam.gov.in.holiday

\*.gov.in.2024.es

\*.cscgov.info

\*.gov.inwww.bteresults.net

\*.gov.in.email

\*.gov.in.holiday

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-21-010**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

email.gov.in.indiagov.pw

www.mes.gov.in.recruitment-circulars.mesce.org

ww25.ww25.mahagov.info

ww25.hcicolombo.gov.inwww.pravasiharyanadivas.in

www.www.www.ftp.cscgov.info

\*.indiagov.pw

\*.cscgov.info

\*.mesce.org

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-TAG-2024-11-21-002**

It has been observed that a recent ongoing cyber-espionage campaign by Insikt Group aka TAG-110, Bluedelta targeted organizations in Central Asia, East Asia, and Europe. The targeted organizations include human rights groups, private security companies, and educational institutions. TAG-110 has been observed deploying the loader HATVIBE and the backdoor CHERRYSPY to conduct operations in this campaign. Initial access is suspected to have come from malicious email attachments or exploitation of vulnerable web-facing services such as Rejetto HTTP File Server (HFS).

Malware used: HATVIBE, CHERRYSPY,  STILLARCH, LOGPIE, Themida

Attack Vectors: Credential Harvesting, Phishing, C&C Server, Scheduled Task, SpearPhishing Attachment, Exploit Public-Facing Application, Malicious File

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

5.45.70.178

212.224.86.69

45.136.198.189

45.136.198.184

**Hashes:**

332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725

d0c3b49e788600ff3967f784eb5de973

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-11-21-009**

It has been observed that APT36 a.k.a. Transparent Tribe is deploying CrimsonRAT, a Remote Access Trojan (RAT) for cyber-espionage activities, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

**Common Features of APT36 Threat Actor:**

* Spear-Phishing (highly targeted and convincing phishing emails to trick victims)
* Information Theft (documents, credentials, and personal data)
* Remote Access
* Credential Harvesting
* Data Exfiltration
* Persistence Mechanisms

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

162.218.211.215

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-21-005**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

31.220.1.88

121.40.26.251

202.95.15.244

178.141.244.152

61.0.11.71

8.222.148.219

45.115.89.45

149.255.15.241

36.107.227.163

120.85.116.125

123.240.198.219

120.85.91.216

123.27.18.191

1.165.122.62

103.149.87.69

103.210.94.242

103.243.232.81

111.255.8.247

112.84.68.231

113.125.114.215

114.220.154.210

117.195.240.30

117.203.54.4

117.235.104.169

117.253.221.125

117.5.147.151

117.72.80.16

117.95.190.179

119.114.51.11

120.85.119.229

120.86.237.234

122.96.31.94

124.95.76.28

125.167.49.151

159.203.87.13

171.22.214.126

175.107.2.53

175.182.218.129

179.43.191.98

182.126.96.100

185.142.53.148

193.239.147.201

193.36.237.126

212.103.50.101

223.13.27.135

26.57.39.131

27.122.61.227

31.133.75.131

31.220.1.88

36.83.127.162

39.144.150.52

43.156.41.165

5.181.86.133

50.3.182.152

59.178.68.224

59.184.248.226

59.89.70.34

59.93.18.2

59.95.80.148

61.3.99.232

64.235.37.140

77.22.233.85

78.37.51.227

88.244.133.151

94.40.250.240

139.180.188.131

206.42.57.228

107.173.210.213

68.69.186.86

120.85.113.206

27.43.206.9

103.199.200.61

123.205.12.113

192.227.180.124

120.85.116.100

114.41.1.230

107.167.122.104

23.105.149.206

1.174.18.248

150.158.20.97

82.156.75.148

120.85.116.115

38.206.131.5

27.43.205.76

103.199.180.62

103.15.254.92

2.56.252.109

77.239.216.203

106.55.137.51

112.94.98.226

120.85.143.228

123.11.209.67

123.5.96.199

120.85.186.192

61.231.237.226

112.175.89.215

103.197.115.61

107.175.31.202

2.59.254.79

2.58.113.117

38.200.6.227

27.122.61.225

173.234.146.157

38.201.195.11

94.156.205.215

23.82.18.125

38.205.188.92

47.95.195.225

93.177.73.171

47.94.13.63

38.206.1.251

103.14.226.142

45.66.231.148

23.228.72.18

107.167.122.105

175.181.100.9

103.214.20.220

47.238.252.193

125.59.46.163

178.72.71.73

190.115.198.110

111.255.33.190

103.137.24.35

120.85.118.246

120.85.183.28

141.148.27.103

47.237.104.189

185.213.83.242

119.129.204.152

209.236.125.59

47.239.11.145

103.167.204.29

27.43.206.6

178.72.76.12

141.98.11.79

185.191.126.248

80.75.212.241

112.94.97.239

62.146.181.8

157.20.146.68

223.149.36.193

223.152.199.34

112.94.98.139

103.199.200.195

77.239.222.228

103.210.94.65

123.204.19.182

45.202.35.24

180.76.184.231

27.43.204.81

42.82.193.57

94.40.215.19

128.14.129.10

45.64.52.160

23.82.18.123

193.176.87.88

37.120.150.84

38.205.190.226

38.205.190.6

142.91.162.231

108.62.50.43

38.204.61.58

175.182.21.76

103.181.90.59

45.202.35.91

183.82.177.217

103.157.112.178

27.111.75.200

120.86.253.183

95.174.94.223

182.44.10.178

103.167.204.45

103.210.94.225

27.43.205.206

120.85.114.110

111.0.84.160

182.44.13.136

195.18.19.104

103.210.94.47

113.172.246.42

89.47.188.121

112.94.97.246

168.220.247.16

103.210.94.116

122.97.138.47

42.51.33.19

120.85.91.19

47.236.61.91

47.236.150.50

36.108.173.25

27.47.3.101

130.61.235.80

120.85.118.124

103.210.94.167

8.222.192.1

120.85.112.185

194.226.169.163

120.85.116.209

47.236.54.136

27.43.204.240

8.222.243.76

8.222.152.112

8.216.121.252

77.239.219.107

103.199.180.74

8.222.168.214

47.237.85.164

103.70.62.20

45.64.105.253

88.198.22.30

23.153.72.133

77.239.214.12

91.107.208.102

120.85.118.200

103.210.94.32

47.245.119.234

120.85.116.149

103.199.180.95

175.107.2.232

113.247.134.46

116.198.243.71

26.77.178.64

45.137.70.156

**URLs:-**

http://103.78.148.243:54794/

http://49.89.165.112:46118/

http://39.80.82.132:39497/

http://61.3.215.209:59734/

http://36.48.28.57:44338/

http://223.220.162.90:50981/

http://219.155.9.98:51198/

http://182.127.166.212:37566/

http://175.151.0.138:39257/

http://149.255.15.30:33421/

http://123.188.95.66:32835/

http://117.255.188.202:33732/

http://117.252.205.223:45265/

http://117.235.124.146:38276/

http://117.209.90.226:35641/

http://115.57.30.0:51819/

http://112.242.156.142:57033/

http://103.15.255.238:51598/

http://112.84.68.231:36704/

http://114.220.154.210:42140/

http://117.195.240.30:37336/

http://117.203.54.4:52241/

http://117.235.104.169:38696

http://117.5.147.151:56526/

http://119.114.51.11:51389/

http://124.95.76.28:42990/

http://171.22.214.126:59976/

http://175.107.2.53:45027/

http://182.126.96.100:56978/

http://185.142.53.148/

http://193.239.147.201/

http://223.13.27.135:41714/

http://39.144.150.52:38901/

http://50.3.182.152/

http://59.178.68.224:39533/

http://59.184.248.226:45517/

http://59.89.70.34:48053/

http://59.93.18.2:50111/

http://61.3.99.232:40820/

http://64.235.37.140/

http://77.22.233.85:34693/

http://78.37.51.227:46349/

http://88.244.133.151:54647/

http://27.17.111.49:57098/

http://175.107.1.107:39584/

http://117.209.31.193:41579/

http://117.208.212.170:56913/

http://115.63.249.36:40081/

http://112.238.89.197:51496/

http://112.248.215.36:39364/

http://103.203.72.26:56418/

http://42.54.111.100:58391/

http://80.246.94.153:39201/

http://102.33.103.87:42607/

http://103.15.255.250:44114/

http://42.58.145.90:39056/

http://42.239.224.201:60479/

http://117.223.6.96:54848/

http://103.200.84.113:56339/

http://42.236.133.205:46822/

http://112.242.156.142:57033/

http://113.27.14.251:40236/

http://113.231.238.219:36333/

http://117.253.221.125:41606/

http://117.235.104.169:38696/

http://221.11.56.146:50919/

http://81.198.225.29:58665/

http://117.209.85.186:58024/

http://59.183.97.101:50355/

http://223.8.210.97:47443/

http://103.197.115.167:57047/

http://117.215.219.22:51719/

http://115.49.147.125:34499/

http://222.138.19.87:46780/

http://223.12.12.193:58796/

http://177.92.240.168:38557/

http://175.107.2.184:57838/

http://60.23.237.57:47468/

http://103.197.115.23:37486/

http://117.198.8.10:32881/

http://120.61.18.59:49188/

http://115.55.196.181:54110/

http://117.222.197.178:49978/

http://175.107.36.81:33971/

http://117.248.63.17:39187/

http://182.121.207.170:49017/

http://123.175.0.253:40825/

http://27.217.147.229:60415/

http://42.178.25.87:51331/

http://210.50.99.52:44683/

http://223.13.67.90:44925/

http://61.1.236.31:42864/

http://200.24.66.50:45345/

http://59.98.139.110:58869/

http://141.195.51.226:48982/

http://117.208.216.228:58872/

http://220.112.30.119:58639/

http://42.227.149.252:56912/

http://125.43.91.244:54010/

http://42.242.86.252:33573/

http://117.253.14.185:50084/

http://27.199.201.130:40141/

http://182.119.214.224:48530/

http://222.139.65.244:59271/

http://103.167.204.63:45297/

http://175.107.0.40:53597/

http://123.235.177.168:50491/

http://27.193.201.31:60383/

http://110.243.28.235:44753/

http://115.52.56.120:58565/

http://117.219.42.81:53231/

http://117.254.99.82:55394/

http://117.209.3.112:60657/

http://172.95.161.66:58553/

http://117.209.239.154:36325/

http://173.16.36.10:55834/

http://117.255.103.117:57063/

http://220.158.158.91:48536/

http://103.200.85.176:52335/

http://117.198.10.106:36032/

http://27.215.85.116:56832/

http://125.45.9.137:38251/

http://123.154.44.41:37040/

http://173.16.36.4:35400/

http://45.230.66.51:11646/

http://27.122.61.195:57058/

http://180.115.74.157:47800/

http://182.116.10.156:41123/

http://115.58.141.104:54022/

http://182.127.33.63:49203/

http://179.164.243.80:53820/

http://117.209.84.96:50593/

http://115.55.23.14:52191/

http://117.222.197.178:49978/

http://69.254.95.4:43611/

http://117.209.88.150:35282/

http://222.188.207.20:40726/

http://59.88.236.4:33166/

http://199.255.181.104:49942/

http://64.235.37.140/bins/

http://117.208.219.23:54563/

http://23.228.72.18/link

http://107.175.31.202/bins/

http://193.239.147.201/bins/

http://223.8.210.187:58823/

http://103.200.85.89:40084/

http://115.56.146.12:55019/

http://117.196.164.42:43784/

http://223.10.1.2:47369/

http://103.203.72.160:49056/

http://222.141.80.112:36052/

http://219.157.238.25:49907/

http://103.78.148.110:51412/

http://103.200.84.114:44120/

http://26.77.178.64:19490/

http://59.97.126.216:55277/

http://115.56.128.218:60368/

http://103.167.205.107:48729/

http://175.107.2.203:47961/

http://182.116.123.200:34573/

http://27.111.75.44:34861/

http://1.70.140.151:43774/

http://59.183.112.252:32803/

http://180.94.33.155:60378/

http://117.211.210.60:41179/

http://117.205.56.126:42684/

http://202.21.42.142:44740/

http://117.198.9.169:56740/

http://87.8.142.30:52910/

http://121.227.78.151:60213/

http://182.106.203.144:43644/

http://61.3.27.1:53941/

http://119.98.163.62:33901/

http://115.50.83.241:55623/

http://110.182.208.194:50198/

http://37.57.155.12:36753/

http://102.33.47.93:58087/

http://223.151.76.23:50204/

http://42.234.165.35:33424/

http://179.172.46.31:55913/

http://103.78.150.165:49300/

http://60.176.0.203:39117/

http://103.200.86.206:36066/

http://117.199.77.78:44400/

http://222.137.112.118:34087/

http://103.200.84.51:60835/

http://27.111.75.206:48415/

http://103.247.52.79:45183/

http://42.231.73.142:53282/

http://139.5.10.155:45985/

http://42.235.128.224:48283/

http://213.40.69.32:46887/

http://59.99.36.191:38112/

http://59.92.160.237:34197/

http://59.88.0.193:44173/

http://117.235.125.6:55417/

http://220.158.158.99:42491/

http://59.99.137.211:52689/

http://110.24.32.11:47407/

http://117.243.221.191:41857/

http://123.173.112.123:35814/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-11-21-010**

Reference is made to earlier advisories on APT SideCopy.

APT SideCopy is known for deploying ActionRAT malware to target individuals and organizations. It aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems.

Adversary is actively targeting government and military officials to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments.

**Common Features of Mythic Malware:**

* Spear-Phishing (highly targeted and convincing phishing emails to trick victims)
* Information Theft (documents, credentials, and personal data)
* Remote Access
* Credential Harvesting
* Data Exfiltration
* Persistence Mechanisms

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

173.212.252.2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-21-006**

The FakeBat campaign, also known as Eugenloader or PaykLoader, is a sophisticated malware attack leveraging malvertising to deliver a malware loader that drops secondary malicious payloads onto victim machines. This attack is notably advanced due to its use of cloaking techniques, evasion strategies, and multiple stages of execution.Here’s a breakdown of the attack:

Initial Access: Malvertising via Google Ads:

Fake Notion Ad: The attackers use a malicious Google ad that pretends to be a legitimate Notion productivity app ad. It appears at the top of search results and is designed to deceive users into clicking on it.

Tracking Template and Cloaking: The malicious ad first redirects users to a tracking template (smart.link) and then to a cloaking domain (solomonegbe.com). This cloaking domain assesses the victim’s system, including geolocation, device type, and browser characteristics, to identify whether the visitor is a real person or a bot. If the victim is deemed legitimate, they are further redirected to a fake Notion site.

Execution: Fake Notion Website

Fake Download: The fake Notion site tricks victims into downloading the FakeBat loader (posing as the Notion app installer).

PowerShell Script: The FakeBat loader executes a malicious PowerShell script (uwrf.ps1) that downloads additional payloads and performs system checks to avoid detection in virtual machine (VM) or sandbox environments. The script also communicates with the attacker's Command and Control (C2) server to send system information and download further malicious content.

Persistence and Further Payloads

Second-Stage PowerShell Script: The initial loader downloads a second-stage PowerShell script, which is responsible for:

Collecting system information (e.g., OS, domain, installed antivirus).

Encrypting and exfiltrating the collected data to the C2 server.

Downloading and executing additional malicious files, including a JAR file.

Obfuscation and Evasion: The JAR file is obfuscated with .NET Reactor and contains an embedded payload that, when executed, injects malicious code into a legitimate Windows process (MSBuild.exe) using process hollowing.

Exfiltration and Data Theft

The second-stage PowerShell script exfiltrates valuable system information, including antivirus software details and OS version, to the attacker's C2 server.

The script also downloads further payloads (such as a RastaMouse AMSI bypass script), which is used to evade detection by Windows Defender and other AMSI-based security tools.

Command and Control(C2)

Throughout the campaign, the attacker communicates with the victim's machine via several external URLs, including the C2 server ghf-gopplrip.com and a Pastebin link that contains additional instructions or code.

Key Features of the FakeBat Campaign:

Malvertising: Fake Notion ads on Google are used to deliver the malware to unsuspecting victims.

Cloaking: A cloaking mechanism evaluates victim systems based on various factors before redirecting them to the fake download site.

PowerShell Execution: The malware uses PowerShell to download and execute malicious scripts, perform system checks, and exfiltrate data.

Evasion Techniques: The malware uses advanced techniques such as process injection and AMSI bypass to evade detection.

Multi-Stage Attack: The malware performs several stages, from initial infection to data exfiltration and payload delivery, each designed to ensure persistence and stealth.

The FakeBat malvertising campaign is a well-structured, multi-layered attack that relies heavily on social engineering (fake Notion ad), evasion tactics (cloaking, PowerShell obfuscation, AMSI bypass), and process injection to deliver malicious payloads. It’s a prime example of a sophisticated loader that targets real users while bypassing common detection methods, making it highly effective for attackers seeking to compromise endpoints without being detected.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

solomonegbe.com

notion.ramchhaya.com

furnotilioin.site/Notion.appx

ghf-gopp1rip.com

rottieud.sbs

relalingj.sbs

repostebhu.sbs

thinkyyokej.sbs

tamedgeesy.sbs

explainvees.sbs

brownieyuz.sbs

slippyhost.cfd

ducksringjk.sbs

**Hashes:**

34c46b358a139f1a472b0120a95b4f21d32be5c93bc2d1a5608efb557aa0b9de

2de8a18814cd66704edec08ae4b37e466c9986540da94cd61b2ca512d495b91a

de64c6a881be736aeecbf665709baa89e92acf48c34f9071b8a29a5e53802019

6341d1b4858830ad691344a7b88316c49445754a98e7fd4a39a190c590e8a4db

**URLs:**

furliumalerer.site/1.jar

pastebin.pl/view/raw/a58044c5

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-21-007**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

92.255.57.58

162.216.149.193

20.118.69.83

18.170.223.246

71.6.134.233

34.78.110.237

147.185.132.221

80.75.212.9

103.95.173.152

114.119.131.28

162.216.150.25

164.90.169.152

162.142.125.84

47.236.242.199

103.42.56.95

35.203.211.13

172.169.4.248

64.62.197.126

64.62.197.133

59.183.131.247

162.243.102.109

59.97.115.60

184.105.139.72

117.208.220.189

184.105.139.68

117.200.191.177

117.254.136.216

59.97.123.44

117.213.125.203

106.219.58.120

18.144.26.200

103.197.115.231

47.237.136.247

123.201.215.240

59.94.121.230

103.171.168.210

52.234.238.185

117.194.213.29

223.190.87.57

117.253.217.98

59.95.85.32

103.240.209.177

45.33.99.215

117.213.253.74

117.255.102.220

117.254.63.100

117.248.173.180

59.182.73.35

117.235.241.248

167.94.138.175

61.0.149.126

117.253.154.247

175.28.32.92

117.248.167.73

117.255.191.138

87.236.176.56

167.94.138.167

117.216.84.116

117.255.209.39

106.222.230.2

103.211.17.67

185.91.127.43

59.98.122.100

117.193.106.73

117.216.240.84

182.78.70.238

194.50.16.198

117.195.149.172

117.248.162.14

117.242.238.194

117.245.245.62

117.206.143.189

220.158.159.189

68.183.42.43

193.163.125.246

67.205.190.232

72.46.130.218

171.51.212.97

59.89.10.155

103.80.22.7

117.221.205.213

61.3.141.65

52.167.144.54

117.221.196.45

103.204.157.120

13.64.108.135

117.254.162.158

103.90.47.186

8.216.87.254

117.235.221.240

117.222.116.134

117.245.94.118

61.0.222.126

59.92.161.162

117.206.76.169

47.251.11.3

35.203.211.203

123.201.215.160

61.3.27.73

61.0.209.69

193.37.32.55

64.62.197.186

122.162.145.85

47.128.60.192

117.211.29.205

59.95.80.46

59.183.161.148

117.194.146.202

120.138.12.25

61.2.109.156

64.62.197.131

64.62.197.123

64.62.197.136

61.0.58.119

59.97.114.60

64.62.197.35

64.62.197.46

59.97.123.85

117.245.43.168

100.33.91.69

47.251.90.213

52.228.152.95

184.105.139.101

206.168.34.42

162.142.125.90

59.93.93.116

117.197.30.94

117.197.62.148

49.205.151.25

117.219.44.77

117.204.198.120

117.216.157.91

152.57.153.58

117.206.135.211

59.91.85.116

47.251.79.51

167.94.138.138

193.163.125.77

92.255.85.110

173.239.211.39

141.98.11.175

47.245.101.101

34.168.125.17

80.85.247.161

92.118.39.214

51.15.114.30

162.216.149.214

20.189.78.65

8.211.51.66

45.115.89.208

64.62.197.67

64.62.197.71

64.62.197.76

79.137.7.69

64.62.197.54

64.62.197.51

117.253.156.154

167.94.138.157

54.193.103.120

65.49.1.16

59.178.43.149

45.138.16.80

65.49.20.100

117.248.161.160

103.51.113.119

59.183.96.247

136.144.35.224

136.144.35.217

162.216.149.33

117.209.240.135

136.144.35.242

117.200.177.205

117.254.97.33

136.144.35.231

117.248.167.196

117.245.37.121

183.97.98.228

59.182.85.10

117.205.167.67

117.208.142.35

117.215.217.157

117.219.123.131

54.72.186.59

206.168.34.174

59.89.30.234

117.253.161.16

117.222.249.26

103.89.170.17

117.235.216.119

117.198.14.211

59.97.126.32

117.216.31.70

117.192.223.137

122.11.212.20

162.216.149.231

149.34.244.136

59.95.84.196

34.83.178.71

147.161.168.113

103.211.17.77

117.248.169.59

59.183.103.37

117.210.189.105

87.236.176.240

59.97.123.115

103.199.180.237

117.223.2.230

117.210.218.104

59.183.112.41

117.254.102.174

59.88.15.174

117.223.7.206

59.178.187.102

59.184.58.9

117.196.173.47

117.254.98.105

59.95.95.169

61.3.16.215

59.97.115.21

117.219.93.198

117.213.80.81

117.252.171.30

59.97.118.66

64.62.197.8

117.254.102.121

117.207.252.83

103.206.251.171

220.233.9.2

59.95.95.63

193.163.125.82

59.183.128.41

210.18.182.186

119.82.94.156

117.196.173.139

59.88.5.195

64.62.197.37

117.223.3.134

116.74.99.14

59.88.152.159

117.207.74.248

59.93.89.94

165.225.231.6

49.207.242.190

117.215.208.11

59.99.218.245

193.37.32.226

170.85.73.6

45.249.164.19

117.209.2.193

117.217.193.102

117.209.124.166

117.219.36.98

117.255.150.122

117.212.189.105

117.195.234.33

59.183.99.228

117.245.38.147

117.235.123.19

117.252.112.251

184.105.247.235

61.0.187.164

87.236.176.249

117.216.154.228

64.62.197.44

64.62.197.42

61.2.235.11

117.235.97.197

117.217.54.125

59.184.49.179

46.101.206.227

117.196.122.106

13.91.166.38

117.221.205.46

59.91.174.6

117.253.8.223

59.92.167.224

117.248.160.69

117.248.162.88

117.245.249.63

117.254.62.206

117.248.19.3

103.158.91.117

94.202.214.45

117.255.185.121

117.254.102.166

162.142.125.94

64.62.197.177

184.105.247.242

117.248.167.195

172.212.61.216

59.91.83.1

66.249.77.33

162.216.149.56

185.91.127.83

34.168.6.238

59.97.112.126

117.248.174.233

117.248.172.22

185.100.54.38

134.122.68.93

87.236.176.109

183.82.52.130

52.157.7.172

64.62.197.19

117.195.92.194

52.42.10.252

170.64.227.209

103.37.80.93

117.212.51.148

117.196.167.254

59.97.124.211

117.253.155.59

172.121.218.184

59.184.255.210

59.178.88.66

185.167.96.146

59.96.240.155

59.184.241.97

117.216.191.53

117.219.34.139

59.182.119.255

106.213.86.7

117.222.113.179

59.97.125.251

117.197.24.61

59.183.8.224

59.184.254.96

117.254.101.241

59.99.214.51

115.124.44.20

59.88.149.138

117.252.99.216

61.1.227.203

117.194.219.118

117.219.87.32

117.212.167.58

74.82.47.4

47.15.248.159

117.248.164.175

35.203.211.232

117.213.245.81

59.183.131.22

117.245.37.122

117.206.70.134

35.203.210.24

59.93.150.73

110.225.174.63

117.209.82.166

59.89.236.126

149.88.103.54

117.248.168.208

54.36.149.73

117.235.242.31

59.99.141.235

59.183.97.114

59.99.217.9

183.82.0.177

92.118.39.115

117.219.187.68

147.185.133.167

52.189.78.44

59.184.40.195

117.216.240.32

137.74.239.156

35.203.211.7

117.253.1.23

59.96.214.168

59.184.254.240

59.96.106.237

152.58.197.150

152.58.123.190

47.250.128.158

152.58.197.47

59.94.46.172

117.223.3.223

117.245.39.157

47.251.110.228

59.178.181.118

92.118.39.37

154.213.187.154

61.3.135.62

152.58.197.214

59.95.94.153

35.203.210.66

152.58.123.82

103.176.152.38

164.52.0.92

117.219.92.156

162.216.149.199

147.161.168.86

106.219.60.142

117.223.7.10

152.58.197.101

45.249.164.46

59.182.91.112

117.209.87.183

185.191.126.248

35.203.210.135

117.195.86.168

103.48.70.81

106.222.233.189

117.217.37.93

91.75.130.30

202.133.55.150

194.32.120.24

117.195.245.47

184.105.247.231

117.252.103.86

59.99.211.42

152.58.123.165

206.168.34.203

54.38.100.149

183.82.3.192

117.252.33.68

117.245.36.10

161.142.151.80

117.195.93.135

27.34.96.54

117.209.127.160

5.180.181.217

104.209.35.185

128.199.59.102

117.253.222.55

117.248.166.117

49.47.2.246

61.3.2.178

117.248.168.231

8.211.52.116

117.211.239.247

64.62.197.181

59.92.82.198

120.61.27.202

47.236.115.10

193.163.125.70

59.99.223.84

162.216.150.147

43.249.184.66

103.55.107.245

198.235.24.243

18.97.5.74

106.222.228.84

13.91.179.188

117.248.173.187

184.105.247.251

193.163.125.231

185.156.46.101

35.203.211.46

61.3.8.39

147.161.167.22

34.82.185.3

35.194.230.235

35.194.140.226

35.189.169.64

34.80.165.120

152.32.170.116

92.118.39.83

103.87.142.243

147.161.217.107

8.219.202.171

64.62.197.154

59.97.123.122

117.204.200.208

117.209.82.236

43.254.204.57

100.25.132.210

54.162.70.136

3.208.18.46

59.99.216.46

220.158.159.64

117.211.239.167

162.216.149.35

61.2.109.41

117.223.3.153

42.111.200.70

162.216.150.112

195.230.103.243

135.148.25.127

223.185.23.137

117.235.25.86

115.179.4.47

117.255.149.224

117.98.0.125

52.90.225.78

54.89.159.37

117.242.202.197

195.230.103.245

117.254.96.129

35.203.210.148

49.206.115.182

117.214.226.211

120.61.29.145

117.195.250.106

59.184.62.190

65.49.1.10

59.89.12.240

117.248.172.29

20.118.69.93

117.196.160.128

117.204.71.182

117.200.152.170

117.243.221.143

149.202.132.194

59.97.118.54

64.62.197.103

117.209.20.96

87.236.176.4

117.214.0.21

61.3.7.188

117.252.162.75

59.184.254.214

117.223.3.165

117.215.218.118

117.211.231.33

42.110.174.221

34.169.108.15

45.33.50.29

45.79.253.156

117.220.62.242

59.96.213.163

59.184.240.221

59.91.24.247

61.1.54.93

117.205.106.15

42.108.74.208

117.245.45.123

117.248.161.215

59.88.231.213

59.95.92.79

117.217.84.10

162.215.129.33

123.201.213.147

62.171.132.30

165.227.47.218

117.255.180.16

103.77.186.234

117.248.165.82

162.214.77.154

59.182.131.88

117.209.6.239

117.212.178.228

110.226.179.16

106.206.225.55

92.118.39.100

178.215.236.240

59.97.121.74

147.185.132.140

14.1.64.25

60.243.25.41

51.8.58.178

49.43.26.54

152.58.199.172

167.94.138.170

59.182.64.247

192.161.189.139

117.215.220.204

59.96.222.35

87.236.176.131

87.236.176.112

117.245.46.168

182.68.75.17

59.93.147.89

45.119.30.231

35.203.211.19

59.178.149.57

64.64.112.21

117.254.100.236

213.230.93.142

117.204.200.125

117.216.172.150

35.203.211.132

117.216.175.158

103.201.134.26

202.148.60.46

192.241.155.120

162.216.150.5

49.34.124.207

162.142.125.80

59.95.80.218

92.118.39.81

103.211.17.105

49.36.191.77

59.97.123.95

59.178.147.231

61.1.79.101

115.247.99.54

5.135.238.155

5.135.238.154

59.184.254.3

13.87.132.36

117.198.11.168

117.223.1.84

162.216.150.251

117.254.98.173

8.211.48.80

117.223.6.134

45.115.89.10

117.253.99.190

92.118.39.36

8.222.162.33

117.217.59.26

59.182.145.241

117.206.183.145

117.248.161.141

165.225.208.79

49.204.115.57

104.207.41.152

48.216.196.105

117.245.43.53

198.235.24.100

5.182.210.124

193.163.125.100

142.93.33.76

167.103.7.90

176.44.94.28

45.79.202.24

117.209.81.123

45.148.10.81

64.23.218.208

125.20.186.118

115.98.171.176

59.89.69.118

117.208.216.185

61.0.185.225

34.19.124.135

170.187.142.131

59.184.249.74

117.210.188.109

117.248.164.124

198.235.24.203

216.218.206.77

47.236.240.124

193.163.125.43

64.62.197.3

162.240.160.35

61.3.110.46

59.89.13.101

45.83.64.138

162.240.226.7

64.226.112.68

117.201.61.235

117.248.170.115

117.248.171.74

117.198.12.178

117.203.57.251

117.195.189.142

167.94.146.25

170.85.6.178

167.94.138.169

120.61.23.245

117.255.185.116

117.205.28.198

159.203.38.16

117.196.173.224

117.198.8.186

117.253.145.153

103.157.163.118

49.36.109.29

219.91.175.18

170.85.56.173

117.219.32.158

34.79.173.164

193.163.125.61

59.88.239.144

45.79.2.59

45.33.118.145

192.241.155.126

161.97.175.164

34.96.46.65

34.96.47.83

34.96.44.179

34.96.46.195

45.79.193.165

117.192.237.223

92.40.199.26

59.97.123.249

117.219.45.26

202.170.205.99

87.236.176.176

49.37.40.144

86.178.63.137

117.195.137.152

117.219.36.175

59.97.127.42

 117.255.183.5

157.51.171.110

59.178.90.139

120.61.232.195

117.248.172.155

8.221.141.224

59.184.54.140

52.189.76.30

193.163.125.60

117.253.164.3

59.97.112.87

193.163.125.235

43.252.103.237

167.94.145.26

45.58.159.225

117.209.18.109

34.168.154.24

18.144.87.170

47.236.7.137

154.90.54.158

35.203.211.65

162.216.150.59

59.97.114.136

45.79.219.12

45.33.42.25

45.33.31.228

59.182.153.185

27.111.75.73

165.154.182.223

61.1.239.40

185.167.97.229

59.182.249.187

206.168.34.133

64.62.197.127

64.62.197.132

27.111.75.194

184.105.247.247

165.225.216.88

59.97.121.249

149.50.212.213

117.222.124.151

106.196.103.105

195.154.200.177

59.97.117.144

117.220.73.81

103.170.64.128

163.53.144.47

45.45.239.22

59.88.12.133

59.178.153.13

34.79.162.0

117.206.189.74

213.180.203.170

35.203.210.181

117.208.26.178

198.235.24.233

59.178.153.20

59.91.67.151

117.209.83.179

117.223.3.190

117.254.174.35

59.97.112.99

220.158.159.103

117.207.248.27

14.195.3.62

117.202.92.145

94.206.13.107

117.213.89.177

45.127.45.176

59.184.51.242

130.61.113.156

117.193.105.176

117.219.87.213

182.69.118.149

59.88.235.11

117.196.121.58

117.248.171.23

59.95.92.31

117.254.162.8

193.163.125.47

185.167.96.138

34.169.11.2

117.213.246.194

117.223.0.203

42.106.241.98

117.200.151.38

117.216.242.240

61.3.131.86

118.194.251.17

117.245.94.124

45.33.84.102

100.33.52.120

173.230.131.181

120.61.12.156

23.239.8.95

45.14.71.18

61.0.176.147

117.196.162.16

117.222.253.105

194.114.136.221

123.201.215.63

110.164.158.29

59.95.94.74

59.92.169.199

167.94.146.17

13.88.19.25

59.184.253.223

117.192.39.50

64.62.197.10

117.195.237.5

148.153.45.234

45.84.107.182

98.80.4.93

52.189.78.91

130.61.181.169

59.93.89.142

117.235.221.228

117.209.47.0

117.251.165.127

117.254.99.30

117.219.174.60

109.177.255.31

117.209.83.206

117.235.27.11

61.0.182.45

59.178.46.193

117.206.180.161

61.0.96.35

220.158.159.110

110.226.182.238

117.206.186.28

117.233.132.174

147.185.133.53

117.208.220.24

117.248.165.141

98.80.4.5

117.248.175.153

59.182.67.213

146.190.197.169

146.70.52.117

103.15.254.202

34.168.94.121

165.154.120.13

117.235.111.213

27.5.23.222

59.91.81.197

61.0.181.230

184.105.247.198

117.235.21.193

117.210.223.19

138.197.134.251

111.90.182.113

104.209.35.59

45.61.135.58

207.46.13.6

104.234.115.45

152.195.205.144

35.216.253.131

172.16.20.13

162.158.107.71

185.13.36.73

13.88.158.175

152.195.205.62

124.156.201.237

143.198.208.51

159.203.84.137

114.119.136.208

103.20.83.105

45.149.241.114

52.26.54.245

54.200.133.41

35.86.177.96

35.89.44.39

143.110.241.189

141.98.168.87

192.3.55.40

139.59.131.151

204.188.228.175

165.225.124.239

152.195.205.115

198.12.114.244

152.195.205.140

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-11-22-005**

It has been observed that LockBit ransomware targeting various Critical Sector Organisations. Lock Bit seeks initial access to target networks primarily through unpatched vulnerabilities, insider access, zero-day exploits etc. On establishing the initial access, it collects network information, and achieves primary goals such as stealing and encrypting data. LockBit attacks typically employ a double extortion tactic. While initiating an attack on the organisations, it has also been observed that attacker first gain the initial access by deploying first stage malware and later use Ransomware-as-a-Service to encrypt targeted system for ransom or permanent denial of the access of the targeted system.

**TTPs :**

* Lockbit demonstrates a formidable capability for autonomously spreading within targeted organizations
* Harnessing tools such as Windows PowerShell and Server Message Block (SMB), among others. Notably, it features a self-propagation mechanism propelled by pre-defined automated procedures, setting it apart from ransomware assaults that rely on manual network infiltration.

**Attack Pattern:**

* Upon compromising an initial host, LockBit swiftly identifies and links with other susceptible hosts, spreading the infection via a script devoid of human intervention. Moreover, LockBit employs sophisticated evasion techniques to circumvent detection by endpoint security systems.
* The combination of autonomous spreading, utilization of native tools, and deceptive file disguises poses significant challenges to the cybersecurity landscape.

**Network Mitigation:**

Network operators are advised to perform mitigation actions, including:

* Patching any identified vulnerabilities associated with LockBit exploits.
* Performing system and operating system updates.
* Conducting network scans using anti-virus software to detect vulnerabilities, intrusions, and lateral movement within the network.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

ww25.lockbit-decryptor.com

**Hashes:**

4274776ecf9e1ded227155eed35505a5

73604c9679fcb4a295b2fb01cccc66ebb50e46d930573f22def87e9234c1fa12

3859ca38ad009d07a156f27de6acbbace281d65471859525eeeb30c553966bbe

202e792ea678490ff6c700cf7d73d67fafa5b9de6603fdd5d1e4905cd34fa08c

8672c0fce7fc66996bf11d3aff03090097c2f6a9f98ea3feb638ad7e04a004aa

82eba2fde3799ac6daa62fafc401daf73aa4b3fb76e77b5c7c0a75ae97d70b57

e539faf9c85283681a4e59219627a744375cc7d4a12e2329a96bc5f77ca674ac

44c5f7d0ad018601def21a24a8ad165ae3f41b0383f9298f71cd5dfac85673db

9657148451103d10808d7fcc89ed4bab0e00912f49c087ca3738867c6fc8951e

07f5e75707521f1aa7ca76c608b79c9e0f4e74b874382b001d00b51f0bd887b5

aec1e4104be794b133abe594a8577a3dd3b69eaef3ae037f5e280e0659fc214a

ade88f211c744d9c4bece3abf640c3ad1b4d73e3a61cca8b39844ad225c9e907

6864095e1e86cd0d813407ca4e42dc6a7e68832a55957ca6ab2f2f2cc23229a7

39aea60c3b78e607c75545e6711375f18d5fb6d024164408e346527272315a37

4f67f4cc5a777b587d4e103f22d22d2e00a476f09011cc35c24843e121cd87d4

353aeb095f66017ae1090d87c2b17f9bd43b2d38c9486d8c65d3a19f1c4b7ef8

7f9f4a055c8d218d719d0c360f60f5d0bceceb0f0beb587c9aae31c0242a1fbd

09eff2690ebc54c4eaf10ccc6c9b9cb0c80699eaf2dbf60de69166ad50c96737

00adf7e31087cb96b8fd6c48b0bc2a9cd01fd7f7718c765196b4a146e8d22247

04d345ef099610e8e4db1cd651c9164fe01095627bdd6870eb667dd0f2077782

df2a9b0f28224bf36128f0a675eb1870712f10ec5404e516ba71c1974e566bd7

0663bf32aec474e7335a55f850ccaf36a7771aa287a797e06e7407a372cae05e

2418d41b9513f6b1e0b67abd76b8e56a53658d5e0cdbf1351d8de4f45b20d240

3e5dcf0d1633ece90628d63e78b9d3901d5ad2267f02749a4f10c67e0250959a

d26fa93c302f11f7b1f38ee162719e7770369cb8bbe113ee5c8175fc17f886a5

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-TAG-2024-11-25-003**

It has been observed that threat actor Earth Kasha, a sophisticated cyber threat actor, is primarily targeting the government, technology, and academic sectors. The recent campaign includes spear-phishing campaigns & exploitation of vulnerabilities in public-facing enterprise applications, notably a heap-based buffer overflow vulnerability [CWE-122] in FortiOS versions & and FortiProxy versions (CVE-2023-27997), Remote Code Execution (RCE) vulnerability in Array Networks Array AG Series & vxAG(CVE-2023-28461) and Remote Code Execution (RCE) vulnerability in Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, and Proself Mail Sanitize Edition Ver1.08 and earlier (CVE-2023-45727). Threat actors utilize legitimate Microsoft tools (e.g., csvde.exe, nltest.exe) to gather Active Directory configurations and credentials post-initial access.

**Impacts:**

Data Exfiltration

**Malware Used:**

LODEINFO is a sophisticated malware family serves as a backdoor for accessing compromised systems, leveraging vulnerabilities in public-facing applications to gain initial access.

NOOPDOOR is a complex backdoor malware which utilizes two communication channels with its command and control (C&C) server, known as active and passive modes, and injects itself into legitimate applications through XML or DLL files.

Cobalt Strike is a commercial penetration testing tool increasingly exploited by threat actor groups to establish remote access through vulnerable Microsoft Exchange servers and web shells like China Chopper.

Mirror Stealer credential dumper targeting multiple applications such as browsers (Chrome, Firefox, Edge and Internet Explorer), email clients (Outlook, Thunderbird, Becky, and Live Mail), Group Policy Preferences and SQL Server Management Studio.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

ns1.tlsart.com

DGA.hopto.org

DGA.gotdns.ch

DGA.myftp.org

DGA.tw8sl.com

DGA.srmbr.com

**Hashes:**

9c681493c81581995e6a48b96411a7004fe77558d7ca863e26398538ad78f385

8574a494425825958c1e978ca7f66a467954fa90c7c898eebac49928519f0eae

87fd4cf002e4d3867462c7a08124cba154750ae78785009a9f213c7479241eef

**IP Address:**

45.76.197.236

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-25-011**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email has attached PDF file ( "Mom held of Defence Secretary Dated 18 November.pdf" ) which is contains a hyperlink ( "https://email.gov.in.indiagov.ws/service/home/?auth=co&id=29238&filename=Ministry%20of%20Defence%20Report%20MoM&charset=UTF-8") with the title "View Document".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URL:-**

https://email.gov.in.indiagov.ws/service/home/?auth=co&id=29238&filename=Ministry%20of%20Defence%20Report%20MoM&charset=UTF-8

**Domain:**

indiagov.ws

**IPs**

45.141.59.180

146.70.142.131

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-25-008**

It has been observed that threat actors are using PXA Stealer, a Python-based malware designed to steal sensitive information, such as credentials saved in browsers, financial data, and cookies. The initial infection begins with phishing emails containing a ZIP attachment that includes a Rust-based loader, obfuscated batch scripts and a decoy PDF. When the loader is executed, it triggers the batch scripts, which open the decoy PDF and run PowerShell commands. These commands then download additional malicious payloads, including the PXA Stealer (a Python package), from infrastructure controlled by the adversaries.

**Various functions performed by PXA Stealer:**

* Kills a variety of processes from a hardcoded list, including endpoint detection software, network capture and analysis process, VPN software, cryptocurrency wallet applications, file transfer client applications, and web browser and instant messaging application processes by executing “task kill” commands.
* Extract the user information, Discord tokens, autofill form data and victim’s credit card information stored in the victim browser database.
* Interact with Facebook Ads Manager and Graph API using a session authenticated via cookies.
* Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
* Hashes:
* fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269
* a9e3f6b9047b5320434bc7b64f4ba6c799d2b6919d41ed32e9815742f3c10194
* e689601d502cc0cd8017f9d6953ce7e201b2dad42f679dc33afa673249ea1aa4
* 782da8904a729971fab86286dd1f44e8de686b7bc66b855079381e1c9e97f6da
* 7db49da15fd159146fe869d049e030a4ecd0d605a762bea4cc4eb702a6ce9ee6
* 707004559c8d625f2d4b296ede702def1f9f52cadf4c52dadc41f3077531d04f
* bc15114841e39203b4e0f5d2cdeef11cc4eceba99eb0c3074a1c6d7b3968404a
* URLs:
* https://tvdseo.com/file/synaptics.zip
* https://tvdseo.com/file/PXA/PXA\_PURE\_ENC
* https://tvdseo.com/file/PXA/PXA\_BOT
* https://tvdseo.com/file/Adonis/AdFnis\_Bot
* https://tvdseo.com/file/PXA/PXA\_PURE\_ENC
* https://tvdseo.com/file/Adonis/Adonis\_Bot
* https://tvdseo.com/file/Adonis/Adonis\_XW\_ENC
* https://tvdseo.com/file/Adonis/Adonis\_Bot0
* https://tvdseo.com/file/STC/Cookie\_Ext.zip
* https://tvdseo.com/file/STC/STC\_XW\_ENC
* https://tvdseo.com/file/STC/STC\_PURE.b64
* https://tvdseo.com/file/STC/STC\_PUP
* https://tvdseo.com/file/STC/STC\_OTO
* https://tvdseo.com/file/PXA/Cookie\_Ext.zip
* https://tvdseo.com/file/STC/STC\_PURE\_ENC
* https://tvdseo.com/file/STC/STC\_BOT
* https://tvdseo.com/file/PXA/PXA\_BOT
* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-25-012**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

certinmail.com

mail-govs.icu

www.email.gov.in.indiagov.ws

www.apply.gov.in.edumartpro.com

www.digitalassam-gov.in.net

\*.indiagov.ws

\*.gov.in.edumartpro.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-RAN-2024-11-25-006**

It has been observed thatm a new ransomware variant named as Helldown is initially focused on Windows systems, but now expanded to Linux and VMware ESX servers. Helldown uses a double-extortion tactic. That means it exfiltrates sensitive information in addition to encrypting the victim's data. It uses secure RSA keys to encrypt files.

Helldown Ransomware primarily spreads through exploiting known vulnerabilities in network devices, particularly Zyxel firewalls. Adversary, Helldown ransomware might be using CVE-2024-42057, a command injection in IPSec VPN that allows an unauthenticated attacker to execute OS commands with a crafted long username in User-Based-PSK mode. Besides these Attackers use phishing emails and malicious attachments to trick users into downloading malicious payload.

**Impacts:**

File Encryption

Personal Information Loss.

Data Exfiltration

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**HASH**

6ef9a0b6301d737763f6c59ae6d5b3be4cf38941a69517be0f069d0a35f394dd

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-25-009**

It has been observed that threat actor groups are targeting the Indian Energy Sector. In their recent attack campaign adversaries are using “ShadowPad” malware as a backdoor to compromised victim entity. The adversary ShadowPad Campaign primarily targets Load Balancer including Proxy Server.

ShadowPad is an advanced modular backdoor designed as the next iteration of PlugX malware. Adversaries are applying this Trojan to deploy malicious payloads, establish and maintain Command & Control (C2) communication and modify plugins.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

95.179.244.134

95.179.141.26

65.20.88.88

139.84.165.29

45.63.41.69

45.32.149.190

208.76.221.246

**Domains:**

madurai.minecraftr.us

remember.publicvm.com

offine.dsmtp.com

kumar123.evils.in

objector.ns01.info

easyes.linkpc.net

linuxes.publicvm.com

musices.longmusic.com

ongc.ns01.info

webday.jumpingcrab.com

offices.dns1.us

gohome.jumpingcrab.com

airport.strangled.net

**Hashes:**

2efefdca63339d7366afa675472090e9f64d78e2aac8e7f0ef0499685f510105

b17af648e89ed9c8596684bd73da432ae4f36dcf4b23ad74b72439ffeb264d4b

07c89ba9f0c67ca0e2b3d81a843582df5d6d917d75c42f9dda6d5c6e58ff291e

25fda4ff44b1bbea60caa78de11a6fe2f807f1e36e25ef055bd1b34a449ee89c

5ba0f3179721e5f6d84936b2e4c8f9fc9b8023678ff8647fe8fa36077b9ce8be

fca010c530d33b642bffaa4e273c4461ede5884e766eb6b4c6f95c0279ead560

9c8e3f1074528e1d8d7bebe48f20f987c8888f49be97ae38104b403451694f1d

91201c03d4249e1505357e50ceee2aa4f90568cb3773da3b926a44980df06f30

47473f6f4aca66e78375d374e035b703e345600e84ffa87ef9b558c18d0f472e

c6950bd6609c50bbd803bdc2c54d0cece8256a2dad2f3a988417c74238bae639

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-26-013**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a hyperlink "https://email.gov.in/?cancel-request", on click, it opens a phishing page with URL "https://mail-govs.icu/", which prompts for username and password of NIC mail account.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URL:-**

https://mail-govs.icu/

**Domain:-**

mail-govs.icu

**IPs:-**

104.21.73.106

188.114.96.3

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-26-009**

Malicious Shadowpad malware, a modular backdoor, IoCs, has been discovered that can infiltrate target systems and provides attackers with capabilities to gather data and control the compromised systems remotely.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

141.164.40.183

139.180.133.22

64.227.184.126

65.20.90.139

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-26-010**

Malicious IoCs of state-sponsored threat actors have been observed which are using foreign-based IP addresses to carry out malicious activities in Indian cyberspace.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

45.76.217.11

164.215.103.248

72.52.178.23

123.58.200.2

94.140.115.117

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-26-011**

It has been observed that a malicious IoC is targeting the Indian Telecom Sector.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

38.92.47.116

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-26-014**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

airports-ecom.gov.in.pagesstudy.com

apaar.education.gov.in.login.ph

bih.gov.in.industries

crsorgi.gov.in.web.lndex.online

gov.in.web.index.php.viewcert.org

gov.inwww.uploadmoon.com

ww25.gov.in.web.lndex.online

ww25.incometaxindiaefilinggov.in

www.crsorgi.gov.in.web.lndex.online

www.punepolice.gov.in.puneparking.com

dc.crsorgi.gov.in.birth.indez.in

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-26-015**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber Threat Actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

cbigov.site

\*.cbigov.site

cbigov-in.cc

cbigov-in.com

cbigov-in.net

cbigov-in.site

cbins.scigv.in

\*.cbigovindia.in

\*.cbigovnews.in

cbigovindia.in

cbigovnews.in

in2024.cbigov.news

in2024.cbigovindia.in

cbigovoffice.in

cbigovin.site

cbigovin.top

cbigovins.top

cbigovins.site

cbigovln.site

cbigov.online

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-27-012**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

79.110.48.149

185.78.76.132

**Domains:**

dkuug.dk

note.gnu.property

**Hashes:**

04273b3ff0a6d04a2e7f1c1ccfb7c99c17b615956b6cc046ecdc18007fbae5df

0b987174964673fda29e59fc0f61111a3a7c07de65e8002e69b0c05a728ab3f8

0c319140825737cb69bb4da52a2641427330b339c966cfd7e97265d61c601338

0f58e36222deb962200e1926808065ffbc281dca1cacb3a9126bfddf860b4c8c

0f85022ce103b3f58e3fa300d7f7aea2fd0e88ddc9b01138dd5b050871e3ed3f

0fb309c0a561329eaac74b747fc5070d69c2e7b02c51dc03292c439cc540754a

0fee9c61d45a0c4afb1d6eeab40d95526897cd5bf5fd8d0632fdf2ff5f9d29d6

12a129a52f33ab77b840ba320865cfd859521ebfd0b2d9488d27f0da38aede56

12ee5849ac6e0233c7d3dd1c034d2de758b5096580b177dd5ec3e50091f8536a

146ab50c1aad8db6bd4d35127e0df0d6fda664615e1b70c50399df6128dc25d7

15935f0d75e08023f6c1d75e38ac6bcc24d4bdb979d795f9947bbae8227b1c2e

180db270ee69630c2b958319cf12d122f385c5ecb5930b2e9b72e00baea2b469

18b17e0c30425b2e4ef1907588dce4eb244f75883c2b8f7a880c3a7718548641

2400c58b92344bc46d0017721988d3d31a95d291e95a8d9ac2df517e9d212752

24f120321016a35854947225f4b3563f97ba520bc3adb2035961266e85bd6d9b

25909dcdaa5a017b5b8a1e5443685684ec8206e0723c314c95aacf85a4ae25b1

28a239b8bbb36f45d82f00aefeb080060d672adf2f3f7d75928c871b3dedf08f

2e2940b45cbef823c911044d428342c6f92f84feb483446dce804599828ed8dc

2e2bdf4bff57b4b4fc5481009e1ce099092df0814b6104e82b4e8ca687e634b3

3271bbdb49f6a5a4ad4cba1256e4805d1ada650f36e0086259bd9ab7d39f4667

3b70d4522353ae89cd92e997e619ad85bfe7c2b0646c70326510be477dbad87c

3d2a7c2d20a403a2db03b94c1ea2d56dd883abfffb4ab5edb4761c57c9440068

3daff116f4970327786e199e3805a1162c673dd65e16f45f18426041417e4a06

40302290da223a90acf43118f60d018b33e302f5f3e51fc9cd48234c39157a48

404a440d37442075abf73182bb8e824832d8376523c9afa6f287ab13b592fbb4

42bd976ddfd6ce5e010bf5dd58a7142ecac418d48e939a6ca66f3568a1b0fac4

434f834b2ae5c247eda402efd05c3758e76de6f4ad8aea4f3ada5bc4bc1308ef

45831451ad219a27adadf9035d8cadb6d190dc87af1c30e5e02aff0316d4b1a3

46101d2ff85c4a3dda7302c9b4dd4116296864799d4211046342005b2582f65e

470b780e17622239f2c95639c8c16bddfbf38290faf2d4613ff52af8c336424f

4871a8c814767184da7a957cab0e207b8179cb751e7f687b03cc6f571d8210a4

4951219e349a20e2278d1fda9fab4941ac5646c134722be8e58df67fe131a841

4dac3b443c6773535d7425e1c042a7959673e9907cdc1fee4cc3158965a3218d

4f099c577ae05f277e0943df7713ed78218bacb6cfaf38b946bcc5919ca72e89

53273563406da096c344a1d7033ef7c23987331a5cc0b7a74c0fa2128cab15c0

57eda45bde69c94d764464315ea613a1b1d426d73fb6ace1845944ff322182f8

58f173143094996f4b73a31709dc8d96c97ef92286b44930d4822662f6937de7

5a02025ae91108bf3f4428986abb7fc72f8f4003a86e9f6eb021c3ab34326a80

5a73d795c30c712b8db3d10d669c23f6f46618696395eb1f1a12682cd3421dfb

5beae4e2f2b9af7fcaeaa58904a050430dba415387dfc1b6d505501ca86b3cd9

5e58519ef638c3de964c83f87f89244ed1d2f086a5675a37573d35bbb11a38b6

5f9c2c08b5f94a34d397e4720a497d8fa49d57a69cc5a52732fdb2306a5c70f9

6003b66232e42e1c119f7d0215a5d45dab016f326f7cde99276463bdbaace2e2

620b1f2818d5b0ab41a1bab7c0f86095aa3dcfe790efa13687a11988536be8b6

62e77536a9b1117df41630e5a916b4e9a831caec4fc922b173bcee9765792df4

641ec1230c385873241373f4a793f7558a71dc5bc86ce6459649cc61294752b6

671616f41516216e51e542c2298988185c0ef5b0a60e91443a96674bc6f6d81c

673723198c0a30b3b45ce35da0408fc49db4682dcd735bf0f27d24a737c004fc

6829ffd81c29e82e311faa06f3f3bbd4f89d39e00d868c87d25cc24809920d65

6b4b86de174ab41ec25c895f4bae3e911600824120560bcef2fa4cfc79f021fd

6fa7c3c95724c0984565b709591a2b73f5715ac1d01e5494fb90a43beaf3091b

71f816a1a3639b90b4b6cfa9541dc77ac5ea404f3c857c80a1074fcbfebabf06

73619cd5815691c451e16add0c9b07df3cdcc85e88885bcbf1f3edb88c13ce9d

7858ac772c297f2b0be0b2013ffb969b5308ef66ab81354612ac152590c81b0a

7994b50959f564dfd69c6cb3b755bd072ef2a297e3111c986213304673c5026b

8104500793d29db762e4a5ab0ed6942a4e4d5823229f3f8122eb6e1bc31dc257

8265970e5c7cd95e2ca59683451928a6942e0b5d2b0b86f838f5fc420bd66216

8319dcb52998be9735de2114f422a2ac35cf5ba1f398201e246a34f8cc148728

8573999d0bb9471d5790f58ab296189829f1333deb6d96795aeae28f3bc9477a

85959e02ee0ff0c16549c63c1094a10b72742a702764dfc7503eecd4e595985f

891123b4a2360ee710ec63ea43af61e4c2136a882afc2de7e592293531292780

8af6f56f604530b29ae55c9f55e8a2c1f0ce30687624552cf4ada9356ff20a9c

8bfab2040d743cc37f4f8e68f5b3b71c4579ef01ed5bf8ea427e80933c22c6a2

8c8c819d2e82d6aa99ff0379a3356198f7ed7affa6593f7b24ec61d60ff665ae

8ea63a0d2aa3caab21b613caa82ab3de3a63a9be1d1760ec696fe6be16bd81d6

8f301c0f38f4e500239339650c29828cff706542471f6676ae6253a34132294c

9003841bb59068e267c3053d27d213db520af70188afdf965768096f273c72e3

91bb48332d371bc9f8bbf9d43c26bb7bc7c848ae298de6b37efd4b25305a93a2

967f61475bce13dceca474b9f631b0d5ce5679024f94eaab9ff3281494fe62c0

984578983cd4e43334510da32a1e34e7ba9230460f380f8b4a9aeba026656367

989bd4fe2d7e2d35beb14f7b579391c0c13542c45d2ff286435a97e507032f78

9dbf43f96b17e948e782d7448e5ad9c5496981bc4013a44289658a26e7f55f20

a20c69480d5a537df1a670c39904d3378d0f116372046434171dca4f600c963d

a4c041a91ce84f64e3fbc4ebe221f9f261a3c951691df8f2dbd0df14055cff81

a52bbe7132e10f076207f55002bb14406f67a6655dcf0b2fa0ed45152e9eb149

a74e5262d990041a4719ee6fb9cf0a245f80c8d5ea4fcc61f570314837a64e4e

acfa300beb99f5f67782628dc96c08653b7e49668d366e913b8e18b22617bd30

af49907e972edf6d0b3ee9b1a72f05321bd090da765f247106f69eb77dca46ff

b06f8a08756d1284bfcbe893381a510bb11665ed0531d7558b6262afde9808d7

b0ebe034fe2828cfca49e0397424daa9c69824349bc70733fdc509223a5dc39b

b1b7c6eade9280800b54d3c46a84fad3f7619ad6145baf316c0c28671fbdf6a9

b2442beb749c1d06a3b9b3be04c72a4a8fd861ead58708af5da818440cf9c37c

b3f51fb861c3153a07097b2f345bc16c7771d570b51ec5a66ad48a48fbb9137d

b5d28104f37a0ca397e3a34a937ecb69adfc4e0791fdc681b60d9e60d9cb57d4

b6893118e0cefc33a548e3e3168bec49dc740e3e623ddb3b0017d0cedee12a34

b83ff8201c52ae77751cc12a447a2a57491c78f0e52288dbeda5f6fb3fe97443

b86398ca187679a7da05419d2e8d6daa0f2afd8d69fb3f3ef4ce79b8925e9c58

ba41774cb78fc93ef7c1fab2a136323839a4461df0a3c61decad14363cd6023d

ba94eff4209adcca3ef281a69bcc0fbf0a7be8dd0df4466bb1d5485e89eaf8b9

bc6e625b293fe7662219c94edc57fd543d159f22e784315a4c6553ef4f8bc2bb

bd21f6dfc15bf8d3d1d2fbaba02e3a0aa04a9896a6800a2e3e1ae3bfe945f041

be8066cfffd1faf1a6973f1f2d12ba939c3c9d214847614e52285b58c73857c1

c39f613330d73fbe16d45c3e0be6bc06b678363f7116a3241176db950ed01fd8

c93a1ca49dbef3543ddab7f009ac740908e7a55986427f8d6fa7ede6887a47ba

caba73ea938c11e80a01fe32c4867ceec23ea270b50bb03f28161f39620f2033

cc3bad70dcc875cb4f367318e8849d0d7f739e90742b35a6361946244a85ebfd

cc73ce5dfd4b16649b88063951b9c5d8dd1bb08d651d46e45a89e702d56d382b

cfb47da714d2c443fa6645c49f82e532c0f273c8db3ba2312cff001e9a3d6a13

d5393d62d801e750004f4a1b8d70af29c724831b4081e1b1b344be913816b0e0

d84cee09eecee93d4e2891f81d470e8b46d1bb3aeb520771983106a5094c5f9a

d950c2f2b4d8d11e6e1ee97bfd4f7d6f09ff07e7d133e089c48053edf50d9a22

dbcd70e6ba1d9ea1a53cdbd3302704c6ef65a863d1ef5587bcafbda710546f3a

dd518786f15cbe017bdd0de430c9c07608710a4973060eb609534bdf32c6d55d

dd8439b0304539bcb0ae03b3d672e9b8ee8ed375d42fc7f37cd55f689dcb9945

e14ff543ebeef75313822124b9f42f1784bb3299118b177986cdb4dfd597a422

e2d2baf676d70d0223a1757fc010ce050cd6386762a0fa17259c03037c8252b2

e34da6630565c0b85f70af451ed359c6eb8bb944d8e5ec97f7fc0bfc38b3982d

e570c8a8726c233836dc5bbe048b155b0b0bfac99045dababf923b0e8e0b34f0

e7b5d3ffa6af42d102fddf8ed94176f384095685265c3d21ec63ed3aaab8ee3b

e809439c34fc80830889fff79410eb1f6250d330b138125ee22289dac18a0282

e94fb4b7a48fb2298d74278833e3ce4aee32219d2a0ef381b1d6867f4bb15696

ee1846029175dd49526680c14db033737a3bb916f9c0c7f80270008a42b984de

eedf3b8d7bddcd100dfb1c6be7da0fc4c3065d7e61cb885ed6c6263e11abff58

efb610328c3089e839d40ad9538e3678de6a1e2168dcd7567d832aac6df58b05

f33f635d366c734cba379f21f1e5598da3ddb0571ee9e8a93aabad658b7edcca

f3a9ec981baedb797ce95d7915c47a2053450d3f749d1cd03788aa6d4189acdf

f447288316a53de2ab2ed6c7f770f3e6b565a6c18fde100748b929ad566f3eca

f5305291fd183cff28ddf026908b3d2193b1b5eef70a5d43d7af1170a06f8ade

f659cb8834c91f1b1110d8fec8a6219775d7da2d91980f182de16da330414230

f681b82ad7228bf9604c21e9397d0c0cf3934418edf3b0774b8ab121d6456f33

f707d2915816eaa0d14dd97d8faabc83896b4ab4baeb6773bae0ef6196856c53

fb06aada76ab0d5ee88a021cccfbc8b68e0a5402da92c2b6cf9709dbb05ff032

fc58fc36161d6bd298547a732161c7c0497f7f7404c38c4e08c3332c4f637067

ff6d8174fcbc91a9595f957104e0accc64bf6ae23094ab0ad79ee15027ac0a1f

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-PHI-2024-11-27-016**

The clusters of activity  has been observed that exploited trusted brands in the transportation sector leveraging fake CAPTCHA-gated phishing pages to manipulate victims into sending money and divulging sensitive personal and financial data. These campaigns were likely opportunistic, as adversaries targeted a wide range of individuals and industries. Adversaries leverage fake CAPTCHAs, multiple redirects, and outstanding bill notifications for small monetary amounts. Adversary to evade detection may change such as the spoofed brand or type of CAPTCHA.

The widespread and ongoing financial theft campaign involving SMS messages that impersonate States Toll-road automatic payment services. The messages sent to individual,  based on spoofed domains in the SMS messages that contain the states’ two-letter abbreviation, for example VA-toll.com  and FL-road.com.  The victims are sent an SMS notification for an outstanding bill that prompts them to visit a spoofed domain for payment.   The phishing messages warns of potential late fees and prompts the victim to pay their bill by hand typing a domain into browser and also contain a logo for the target’s local payment service. When the victim visits the domain, they are required to solve an image-based CAPTCHA custom made by the threat actor. Then, victims are redirected to a page with the toll services’ logo that prompts the user to input their name and ZIP code to view their bill. Any input will generate the same notification, the victim’s name is auto populated at the top and the message states that they owe chares mentioned in the bill and will incur fine charge if they do not pay immediately. If the victim clicks the “Proceed Now” button, they are taken to a final page that prompts them to input their name, address, phone number, and credit card information.

Adversary’s malicious activity heavily relied on brand impersonation — malicious content that closely resembles a trusted brand, like a company's logo or email format. This is a common technique used to trick users into clicking on malicious links or attachments or divulging sensitive data. Mimicking common legitimate behavior can also evade some Endpoint Detection and Response (EDR) systems that rely on signature databases to identify abnormal email content and activity.  Threat actors have continued these types of scams but coupled brand impersonation alongside CAPTCHA-protected phishing pages likely to add another layer of obfuscation to ensure the malicious content reaches victims.

Threat actors leveraging three types of CAPTCHAs:

* Legitimate: Threat actors register legitimate CAPTCHAs, such as Cloudflare’s Turnstile and Google’s reCAPTCHA, to hide phishing pages
* Spoofed: Threat actors create and control CAPTCHAs that impersonate legitimate brands.
* Custom: Threat actors create and control CAPTCHAss that do not impersonate any brand.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domains:**

wa-gtg.com

goodtogo-wa.com

wagood-togo.com

gtgwa.com

mygood-2go.com

tollwa.com

wagtg.com

ws-gtg.com

ws-dot.com

fl-road.com

fl-pass.com

pass-fl.com

tx-account.com

tx-road.com

oh-route.com

link-pa.com

lane-pa.com

plate-pa.com

gov-pa.com

pa-plate.com

ilroad.com

iltolls.com

va-route.com

ezp-va.com

va-toll.com

toll-va.com

va-ez.com

va-lane.com

ks-lane.com

ks-drive.com

lane-ks.com

Afrikagazetesi.info

gkadillak.com

**IPs :**

82.147.88.22

45.152.115.161

13.248.213.45

**URL**:

https[:]//tx.gl/r/jQ2HG/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-11-27-011**

Reference is made to earlier advisories on APT SideCopy.

It has been observed that APT Sidecopy is targeting Indian Government. Please find below IOCs in this regard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

45.202.35.172

**URLs:-**

http://email.gov.in.indiagov.ws

http://email.gov.in.indiagov.pw

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-11-27-012**

**Palo Alto Networks Released Security Updates**

Palo Alto Networks has released security updates to resolve an authentication bypass vulnerability in the Management Web Interface. The affected versions are PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2 software on PA-Series, VM-Series, and CN-Series firewalls and on Panorama (virtual and M-Series) and WildFire appliances.

CVE ID: CVE-2024-0012 (Critical)

**Vulnerability in Cesanta Mongoose Web Server**

Use of an out of range pointer offset vulnerability has been discovered in Cesanta Mongoose Web Server. The affected version is Cesanta Mongoose Web Server v7.14.

CVE ID: CVE-2024-42383 (Critical)

**Vulnerability in Synology BeePhotos**

A command injection vulnerability has been discovered in the Task Manager component of Synology BeePhotos. The affected versions are Synology BeePhotos before 1.0.2-10026 and 1.1.0-10053 and Synology Photos before 1.6.2-0720 and 1.7.0-0795.

CVE ID: CVE-2024-10443 (Critical)

**Vulnerability in Apereo CAS**

An improper authentication vulnerability has been discovered in Apereo CAS. The affected version is Apereo CAS 6.6.

CVE ID: CVE-2024-11209 (Critical)

**Vulnerability in D-Link**

A buffer overflow vulnerability has been discovered in D-Link. The affected version is D-LINK DI-8003 v16.07.26A1.

CVE ID: CVE-2024-52759 (Critical)

**Automated Logic Released Security Updates**

Automated Logic has released security updates to address multiple vulnerabilities in its equipment- WebCTRL Premium Server. The affected versions are Automated Logic WebCTRL server version 7.0, Carrier i-Vu version 7.0, Automated Logic SiteScan Web version 7.0 and Automated Logic WebCTRL for OEMs version 7.0.

**mySCADA's Equipment  Security Updates**

mySCADA's Equipment has released security updates to resolve multiple vulnerabilities in myPRO. The affected versions are mySCADA myPRO Manager versions prior to 1.3 and mySCADA myPRO Runtime versions prior to 9.2.1.

CVE ID: CVE-2024-47407 (Critical), CVE-2024-52034 (Critical), CVE-2024-45369 (High), CVE-2024-47138 (Critical), CVE-2024-50054 (High)

1. **VA-2024-11-28-013**

A zero day "Missing Release of Resource after Effective Lifetime" vulnerability tracked as CVE-2024-20481 affects Cisco Firepower Threat Defense (FTD) Software and Cisco Adaptive Security Appliance (ASA) Software.

The Remote Access VPN (RAVPN) service's resource exhaustion is the cause of the vulnerability. This vulnerability can be exploited by an unauthenticated remote attacker by flooding an affected device with VPN authentication requests.

A successful exploit can use up all available resources, which would cause the RAVPN service on the compromised device to be denial of service (DoS).

Reloading the device might be necessary to restore the RAVPN service, depending on the severity of the attack.

Following are the products that are NOT affected by this vulnerability:

1. IOS Software

2. IOS XE Software

3. Meraki products

4. NX-OS Software

5. Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software

**Threat Type**: Vulnerability

(CVE-2024-20481)

CVSS SCORE-5.8

**IMPACT:**

1. Denial of Service (DoS): The RAVPN service may be interrupted, and in order to restore functioning, a device reload may be necessary.

2. Resource Exhaustion: If the attack uses up all of the system's resources, performance may suffer or the service may stop entirely.

**MITIGATIONS AND RECOMMENDATIONS:**

1. Patching CVE-2024-20481: Prioritize patching this vulnerability right away to protect against potential intrusions and system breaches because of its critical nature, active exploitation in real-world settings, and potential serious effects on the company's assets.

2. Update Software: Ensure all affected Cisco ASA and FTD devices are updated with the latest software patches from Cisco to address this flaw, CVE-2024-20481.

3. Turn on logging, set up threat detection for VPN providers that allow remote access, and implement hardening techniques including turning off AAA authentication and manually blocking unauthorized connection attempts.

4. Monitor VPN Traffic: Keep an eye on VPN traffic for unusual patterns that may indicate an attack.

5. Implement Security Measures: Use firewalls and intrusion detection systems to help detect and block malicious activities.

6. Monitor VPN Traffic: Keep an eye on your Remote Access VPN traffic for unusual patterns or high volumes of authentication requests that could indicate an attack.

7. Rate Limiting: Implement rate limiting on authentication attempts to reduce the risk of resource exhaustion and denial-of-service attacks.

8. Intrusion Detection Systems (IDS): Use IDS to detect and alert on suspicious activities and potential attacks targeting your VPN services.

9. Firewalls and Access Controls: Strengthen your firewall rules and access controls to limit exposure of your VPN endpoints.

10. Network Segmentation: Segment your network to limit the impact of a potential breach. Ensure critical systems are isolated from less secure segments.

11. Regular Security Audits: Conduct regular security audits and assessments to identify and mitigate vulnerabilities in your network infrastructure.

12. User Education: Train users on best practices for security, including recognizing phishing attempts and using strong, unique passwords.

13. Incident Response Plan: Have a robust incident response plan in place to quickly respond to and recover from security incidents.

14. Backup and Recovery: Regularly back up your configurations and critical data. Ensure that backups are secure and can be restored quickly in the event of an attack.

1. **TA-PHI-2024-11-28-017**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a hyperlink with the headline "Annual-Leave-Compliance-Report-2024.pdf", on clicking the hyperlink, it opens a phishing page with a phishing page with the URL  "https://agenciavivancy.com.br/5gWuL/update.html#dg.dgaqa@nic.in", in which the email ID of the target is auto-filled and it asks for password of the email ID.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**URL:-**

https://agenciavivancy.com.br/5gWuL/update.html#dg.dgaqa@nic.in

**Domain:-**

AgenciaVivanCy.com.br

**IPs:-**

192.185.131.99

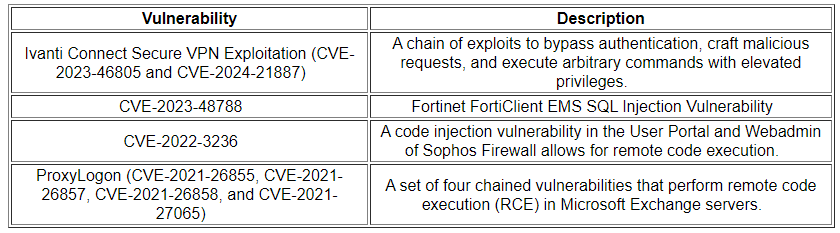
151.101.66.159

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-11-28-012**

It has been observed that state-sponsored APT Earth Estries (aka Salt Typhoon, FamousSparrow, GhostEmperor and UNC2286) has emerged as one of the most aggressive Advanced Persistent Threat (APT) groups, primarily targeting critical industries such as telecommunications and government entities. The APT uses a new backdoor, GHOSTSPIDER, modular backdoor SNAPPYBEE aka Deed RAT, a cross-platform backdoor named MASOL RAT-based on its PDB string and another tool shared among APT groups.

For initial access, Earth Estries is aggressively targeting the public-facing servers of victims by exploiting server-based N-day vulnerabilities, including the following:



After gaining control of the vulnerable server, we observed that the attackers leveraged living-off-the-land binaries (LOLBINs) like WMIC.exe and PSEXEC.exe for lateral movement, and deployed customized malware such as SNAPPYBEE, DEMODEX, and GHOSTSPIDER to conduct long-term espionage activities against their targets.

Brief description about these backdoor malwares is as follows:

1. GHOSTSPIDER-

GHOSTSPIDER is a sophisticated multi-modular backdoor identified during attacks targeting Southeast Asian telecommunications companies. Key features include:

Modular Design: GHOSTSPIDER can load different modules tailored for specific purposes.

Secure Communication: It communicates with its command and control (C&C) server via a custom protocol secured by Transport Layer Security (TLS).

Long-Term Targeting: The backdoor has been utilized in prolonged attacks against government entities and service providers since at least 2020.

Related Threat Groups: Some tactics used by GHOSTSPIDER overlap with those of other APT groups like FamousSparrow and GhostEmperor, although direct attribution remains uncertain.

C&C Infrastructure: Recent findings include GHOSTSPIDER’s C&C infrastructure linked to potential ransomware operations, indicating its use for both espionage and financial gain

2. SNAPPYBEE

SNAPPYBEE, also known as Deed RAT, is another backdoor deployed by Earth Estries. Its characteristics include:

Deployment: SNAPPYBEE was detected in operations targeting government entities, with specific samples found in compromised systems in October 2024.

Shared Tools: It is considered to be a tool shared among various Chinese APT groups, indicating it may not be exclusive to Earth Estries.

Identification: It was linked to the ZINGDOOR attack chains, showcasing its role in complex cyber-attack scenarios

3. MASOL RAT

MASOL RAT is a cross-platform backdoor that has been linked to Earth Estries with a focus on Southeast Asian government networks. Important points include:

Initial Discovery: MASOL RAT was first identified in 2020 during investigations into government-targeted incidents.

Deployment on Linux: The backdoor has been specifically observed targeting Linux devices within government networks.

Limited Attribution: Although MASOL RAT has been associated with Earth Estries, there is still low confidence in linking it to specific exploits without further evidence

4. DEMODEX ROOTKIT

The DEMODEX rootkit plays a significant role in Earth Estries' cyber strategy, enabling them to conduct extensive and persistent attacks on their targets. The group's advanced methodologies and adaptability highlight the ongoing threat posed by sophisticated APTs in the current cyber landscape.

Continued monitoring and analysis will be essential to understand the full extent of their operations and develop countermeasures against such persistent threats.

**IMPACTS:**

The impacts of these cyber intrusions can include:

* Data breaches leading to loss of sensitive information.
* Financial losses due to operational disruptions.
* Damage to organizational reputation.
* Legal implications arising from data protection violations.
* Compromised intellectual property.
* Increased costs related to incident recovery.
* Potential for further attacks if initial breaches are not contained.
* Erosion of customer trust in affected organizations.

**DISTRIBUTION:**

The malware has been distributed through:

* Exploitation of known vulnerabilities (e.g., CVE-2022-3236, CVE-2023-46805, CVE-2023-48788).
* Phishing emails containing malicious attachments.
* Malicious downloads from compromised websites.
* Supply chain attacks targeting third-party vendors.
* Use of social engineering to trick users into executing malware.
* Infected USB drives used in targeted environments.
* Remote access tools that facilitate unauthorized access.
* Custom scripts designed to deliver payloads undetected.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Hashes: SHA-256**

fc3be6917fd37a083646ed4b97ebd2d45734a1e154e69c9c33ab00b0589a09e5

fba149eb5ef063bc6a2b15bd67132ea798919ed36c5acda46ee9b1118b823098

2fd4a49338d79f4caee4a60024bcd5ecb5008f1d5219263655ef49c54d9acdec

16c8afd3b35c76a476851f4994be180f0cd72c7b250e493d3eb8c58619587266

9ba31dc1e701ce8039a9a272ef3d55aa6df66984a322e0d309614a5655e7a85c

25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b

6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc

b2b617e62353a672626c13cc7ad81b27f23f91282aad7a3a0db471d84852a9ac

05840de7fa648c41c60844c4e5d53dbb3bc2a5250dcb158a95b77bc0f68fa870

1a38303fb392ccc5a88d236b4f97ed404a89c1617f34b96ed826e7bb7257e296

**IPs:**

103.91.64.214

165.154.227.192

23.81.41.166

158.247.222.165

172.93.165.14

91.245.253.27

103.75.190.73

45.125.67.144

43.226.126.164

172.93.165.10

193.239.86.168

146.70.79.18

146.70.79.105

205.189.160.3

96.9.211.27

43.226.126.165

139.59.108.43

185.105.1.243

143.198.92.175

139.99.114.108

139.59.236.31

104.194.153.65

**Domains:**

materialplies.com

news.colourtinctem.com

api.solveblemten.com

esh.hoovernamosong.com

vpn114240349.softether.net

imap.dateupdata.com

pulseathermakf.com

www.infraredsen.com

billing.clothworls.com

helpdesk.stnekpro.com

jasmine.lhousewares.com

private.royalnas.com

telcom.grishamarkovgf8936.workers.dev

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-11-28-014**

A "Missing Authentication for Critical Function" vulnerability tracked as CVE-2023-28461 exists in Array Networks AG/vxAG secure access gateways is being exploited widely.

Using a flags attribute in an HTTP header, an attacker can access the SSL VPN gateway's filesystem without requiring authentication. A vulnerable URL might then be used to exploit the product.

Threat Type: Vulnerability

CVE-2023-28461

CVSS SCORE-9.8

Severity: High

Associated Malware Families-  MirrorStealer and LODEINFO

Associated Threat Actor- Earth Kasha

Affected Version:

1. Array Networks Array AG Series and vxAG (9.4.0.481 and earlier)

2. The vulnerability has NO impact on AVX, APV, ASF and AG/vxAG (running ArrayOS AG 10.x versions) series products.

3. For Array AG/vxAG series products running ArrayOS AG 9.x versions, attackers may exploit this vulnerability without authentication.

**IMPACT:**

1. Unauthorized Access: Attackers can gain unauthorized access to sensitive files and data on the affected devices

2. Remote Code Execution (RCE): The vulnerability allows attackers to execute arbitrary code on the affected devices, potentially leading to complete system compromise

3. Data Exfiltration: Sensitive data can be stolen and exfiltrated to remote servers controlled by the attackers

4. Service Disruption: Exploitation can disrupt essential services, leading to downtime and operational challenges

5. System Compromise: The attacker can gain full control over the affected system, posing a significant threat to the security and integrity of the network

**MITIGATIONS AND RECOMMENDATIONS:**

1. Apply Security Patches: Update your Array Networks AG and vxAG ArrayOS to version 9.4.0.484 or later, as this patch addresses the vulnerability.

Prioritizing patching this issue by following vendor mitigation instructions is crucial. If mitigations are not practical, product discontinuation may be an option. Unauthorized access and serious system harm could result from ignoring this vulnerability.

2. Disable Vulnerable Features: Temporarily disable functionalities such as Client Security, VPN client automatic upgrades, and Portal User Resource

3. Implement Blacklist Rules: Set up blacklist rules to filter out malicious traffic targeting the vulnerable URLs.

4. Network Segmentation: Segment your network to limit the spread of an attack and protect critical systems.

5. Monitor System Logs: Keep a close eye on system logs to detect any unauthorized access attempts or other suspicious activities

6. Intrusion Detection Systems (IDS): Use IDS to detect and alert on any unusual activities targeting the affected devices

7. Regular Security Audits: Conduct regular security audits and assessments to identify and mitigate vulnerabilities in your network infrastructure.

8. User Education: Train employees on recognizing phishing attempts and following best security practices to reduce the risk of initial access.

1. **TA-MAW-2024-11-28-013**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP Addresses:**

120.86.254.64

192.145.127.218

120.86.238.253

205.185.122.99

107.167.122.105

5.35.104.31

103.199.180.151

121.15.197.24

202.43.120.248

103.110.33.164

45.137.70.156

107.175.31.202

45.202.35.91

193.239.147.201

1.163.222.145

120.85.112.255

120.86.254.189

64.235.37.140

154.213.184.14

95.214.53.205

103.78.150.62

45.115.88.133

120.85.93.199

45.115.88.135

193.143.1.70

103.210.94.75

157.211.68.144

31.220.1.88

27.157.145.215

122.194.9.231

219.71.85.54

162.158.179.77

59.182.126.249

112.25.237.54

117.205.20.133

217.160.89.196

178.92.21.68

36.49.65.210

172.71.214.168

172.71.215.13

103.247.7.224

175.107.3.5

85.122.180.176

117.209.29.120

103.15.254.153

103.149.87.69

102.33.43.172

154.216.17.126

112.64.45.170

103.210.94.105

82.112.227.1

220.198.241.125

103.208.230.102

77.239.211.133

89.22.230.162

185.208.207.3

36.41.184.119

123.241.105.30

47.103.52.14

116.198.224.56

61.58.86.207

117.209.84.95

183.88.213.128

223.10.49.12

47.236.52.187

47.84.32.175

47.236.252.254

8.222.226.153

112.232.241.7

8.219.237.171

47.237.118.0

47.236.136.217

117.209.81.151

120.85.118.237

47.237.6.119

47.237.115.171

47.237.132.148

47.236.235.24

8.222.197.183

8.222.137.97

47.236.51.1

103.146.40.5

47.237.126.189

47.236.50.100

178.128.95.87

47.236.232.202

58.47.107.175

47.84.69.78

117.217.142.223

8.222.183.247

102.212.40.131

5.187.85.84

8.222.148.63

47.84.34.226

117.208.103.216

77.239.222.52

219.70.181.86

190.77.64.35

220.158.158.241

130.61.39.54

103.210.94.189

124.235.238.245

8.222.143.176

58.59.153.213

117.209.33.153

117.254.182.209

59.99.199.37

110.182.125.78

120.86.254.139

103.15.255.126

77.239.211.30

27.111.75.236

47.236.231.80

8.222.197.158

120.85.115.111

202.129.16.23

171.43.135.58

206.1.12.240

120.85.119.55

47.237.133.252

27.43.206.41

47.237.24.160

103.229.81.122

182.44.8.100

171.36.176.161

103.109.101.6

120.85.118.13

141.164.107.3

8.222.160.183

103.210.94.53

27.43.204.179

8.222.166.37

8.222.172.249

120.85.114.247

27.122.61.216

153.192.54.94

120.85.117.6

47.236.168.202

27.47.3.51

154.216.20.88

**URLs:-**

http://103.167.205.33:52687/

http://117.209.81.139:42022/

http://117.209.80.168:57191/

http://115.55.195.165:39289/

http://117.81.26.204:52509/

http://117.235.122.31:49080/

http://175.107.0.237:38916/

http://103.151.46.128:39152/

http://27.122.61.185:47870/

http://103.197.115.111:38366/

http://59.97.114.139:34061/

http://77.247.88.84:50223/

http://103.203.72.87:38476/

http://117.235.156.133:49044/

http://45.230.66.4:11451/

http://26.99.153.102:19490/

http://72.175.25.81:47405/

http://59.99.207.146:35906/

http://175.107.0.71:38189/

http://110.183.30.55:38946/

http://117.242.131.107:47720/

http://59.89.194.96:56689/

http://110.86.188.198:56946/

http://196.189.152.103:33694/

http://117.223.6.196:55760/

http://120.57.220.188:55812/

http://27.216.118.69:40600/

http://223.8.49.30:54512/

http://59.182.129.205:35222/

http://103.199.200.237:37986/

http://182.112.60.93:60398/

http://175.107.36.6:59582/

http://89.200.227.78:35189/

http://27.111.75.41:49139/

http://112.64.155.152:54693/

http://103.15.254.151:40132/

http://112.248.244.139:57974/

http://117.193.133.234:56637/

http://103.200.85.244:57202/

http://117.209.88.66:56205/

http://27.202.227.227:55412/

http://222.188.235.60:35921/

http://59.89.192.126:54443/

http://220.158.158.117:46317/

http://103.15.254.153:54129/

http://157.211.68.144:44713/

http://27.157.145.215:59018/

http://102.33.43.172:38584/

http://219.71.85.54:40527/

http://112.64.45.170:50000/

http://59.182.126.249:39620/

http://112.25.237.54:34677/

http://117.205.20.133:56658/

http://178.92.21.68:51426/

http://36.49.65.210:45611/

http://103.247.7.224:53775/

http://175.107.3.5:57290/

http://117.209.29.120:39034/

http://58.47.107.175:44916/

http://190.77.64.35:37541/

http://117.208.103.216:48044/

http://59.99.199.37:59509/

http://58.59.153.213:43895/

http://5.187.85.84:6108/

http://223.10.49.12:44164/

http://219.70.181.86:58411/

http://124.235.238.245:59257/

http://117.254.182.209:49834/

http://117.217.142.223:45634/

http://117.209.84.95:59722/

http://117.209.81.151:36522/

http://117.209.33.153:36444/

http://112.232.241.7:41111/

http://110.182.125.78:45097/

http://103.15.255.126:54944/

http://103.197.115.201:49351/

http://220.158.159.159:51834/

http://117.209.83.226:36030/

http://42.229.237.50:58844/

http://202.169.234.51:35003/

http://117.206.179.224:45172/

http://220.158.158.165:43050/

http://103.203.72.253:46473/

http://117.195.249.6:42583/

http://120.61.244.93:40563/

http://125.43.82.32:52840/

http://117.209.94.246:44074/

http://192.21.160.65:50116/

http://220.158.159.213:34158/

http://115.53.232.132:53711/

http://42.237.107.21:60810/

http://103.200.84.59:58011/

http://117.209.84.194:36965/

http://222.141.37.133:50907/

http://103.15.254.171:58844/

http://45.115.89.219:59660/

http://117.217.37.92:39011/

http://220.158.158.181:48876/

http://117.209.95.208:56178/

http://177.163.245.94:34303/

http://103.197.115.168:37081/

http://103.15.254.67:38653/

http://117.213.88.228:41708/

http://117.209.93.189:39882/

http://59.95.129.105:37229/

http://59.89.5.136:49118/

http://123.4.70.197:38490/

http://220.158.158.153:52796/

http://120.61.206.85:46094/

http://113.27.34.180:40245/

http://223.8.194.185:46348/

http://25.8.130.149:19490/

http://115.63.11.93:58761/

http://117.209.47.34:56104/

http://117.213.248.7:36301/

http://223.15.53.106:48394/

http://61.0.182.148:43861/

http://45.229.174.165:56286/

http://103.203.72.229:54646/

http://125.44.241.137:48812/

http://220.158.159.152:51068/

http://171.36.177.94:10058/

http://117.222.197.178:49978/

http://59.89.71.147:41513/

http://117.209.81.97:33618/

http://103.247.54.185:56234/

http://117.235.32.249:60498/

http://59.182.88.140:43643/

http://123.10.138.70:48574/

http://139.5.10.191:35943/

http://61.1.233.57:45066/

http://180.115.170.102:57184/

http://117.211.209.14:56009/

http://117.222.112.189:35471/

http://58.47.122.248:49008/

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-MAW-2024-11-29-014**

A compiled list of tunneling tools is attached that are leveraged by state-sponsored/ ransomware actors, along with Tunnel Detection Mechanism & Mitigation for due consideration.

**File Name:** Tunneling\_tools.pdf

**SHA256:** 4bd00e63596fc657a5de019614c33ec425ccfe5a2c62a465bfb96402b719a2e0

**Reference:** CERT-IN [CMTX-P-TL-1120243214]

1. **TA-MAW-2024-11-29-015**

ASYNCRAT, a backdoor written in .NET, uses a unique binary protocol to communicate over TCP. The backdoor has the ability to run shell commands and download plugins, which may be kept in the registry or run immediately in memory. The downloaded Plugins can add features like file transfer, keylogging, video recording, screenshot capture, and cryptocurrency mining. Additionally, ASYNCRAT provides a plugin that targets login credentials kept by web browsers running on Chromium and Firefox. Adversary after execution, establishes communication with the Command & Control (C2) server and allows remote control of the compromised systems.

**Impacts:**

* Remotely control of the compromised systems.
* Execute remote commands, Log keystrokes, Exfiltrate data and deploy additional malware.
* AsyncRAT can be used to spread laterally across the network, potentially infecting other systems and creating a broader security breach.
* AsyncRAT often includes features to evade detection and maintain persistence in the infected system, making it challenging to remove and recover from the infection.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

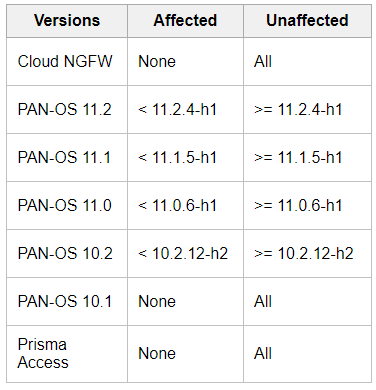
147.185.221.23

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **VA-2024-11-29-015**

t has been observed that in a malicious activity, threat actors are exploiting an authentication bypass vulnerability (CVE-2024-0012) & privilege escalation vulnerability (CVE-2024-9474) in the Palo Alto Networks PAN-OS Operating system. When combined, these vulnerabilities allow attackers to bypass authentication and gain root access to the affected devices, potentially compromising entire networks. The activity of exploiting these vulnerabilities, referred to as Operation Lunar Peek. After successful exploitation, adversaries drop malware and execute commands on compromised firewalls.

The vulnerabilities affected the following firewall models and their versions:



\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP address**

91.208.197.167

104.28.208.123

136.144.17.146

136.144.17.149

136.144.17.154

136.144.17.158

136.144.17.161

136.144.17.164

136.144.17.166

136.144.17.167

136.144.17.170

136.144.17.176

136.144.17.177

136.144.17.178

136.144.17.180

173.239.218.248

173.239.218.251

209.200.246.173

209.200.246.184

216.73.162.69

216.73.162.71

216.73.162.73

216.73.162.74

**Hash (SHA256):**

3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*